May 2022

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

SASHA ROMANOSKY, JONATHAN W. WELBURN

Disclosure of Software Supply Chain Risks

The nation's reliance on computer software to run and manage critical business services has increased dramatically over many decades and only continues to grow. But with this reliance comes risk. The increasing rate of and impact from the exploitation of software vulnerabilities has caused billions of dollars of damage and losses to thousands of companies across the world. And the malicious compromise—or even accidental failure—of software threatens firms across all industries throughout the United States. For example, the NotPetya and WannaCry ransomware attacks caused tens of billions of dollars of losses globally, and the disclosure of the software vulnerabilities Heartbleed in 2014 (Lee, 2015) and log4j in 2021 (Tan, 2022) affected hundreds of millions of devices. The compromise of the SolarWinds software in 2019 (Greig, 2022) became a potent reminder of the fragility of the U.S. dependence on modern software applications and of the potential harms to corporate balance sheets, customer data, and sensitive government records.

Moreover, an increasing number of modern software applications are being built on a foundation of third-party and open-source software components, developed by thousands of professional and volunteer contributors across the world. This complexity and decentralized nature of the modern software ecosystem mean that firms are becoming more separated from the oversight of the software that runs

RAND
CORPORATION

their business and increasingly exposed to risks because of this expanding software supply chain.

In March 2022, U.S. Securities and Exchange Commission (SEC) Chair Gary Gensler stated, "Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks" (SEC, 2022). In this Perspective, we build on this cybersecurity risk and argue that, although the SEC has taken some measures to incentivize proper disclosure of cyber risks, software supply chain risks are an important yet overlooked concern.

Recognition of the Importance of the Software Supply Chain Is Growing

In 2018, the House Energy and Commerce Committee stated that "[open-source software] is such a foundational part of the modern connected world that it has become critical cyber infrastructure" (House of Representatives, Energy and Commerce Committee, 2022).

Abbreviations

IT	information technology
NIST	National Institute for Standards and Technology
SBOM	software bill of materials
SEC	U.S. Securities and Exchange Commission
Y2K	Year 2000

In recent years, two separate initiatives, led by open-source consortiums and security software companies, have prompted the collection of data and publishing of reports that unveiled the vastness and prevalence of open-source software usage through U.S. businesses and the intricate dependencies among these products (Veracode, 2020; Nagle et al., 2020). For example, Veracode, a software analysis company, has observed that software applications are reducing in size but exploding in the number of distributed packages, making the overall management and security much more complicated. In addition, the Core Infrastructure Initiative, an open-source consortium of researchers and software manufacturers, argues that the decentralized and voluntary manner in which open-source software is written and distributed means that there is often no oversight of software quality or maintenance (Nagle et al., 2020).

In addition, Executive Order (EO) 14028 was released in response to the White House's recognition of the dire state of cybersecurity across federal agencies. Section 4 of that order specifically addressed software supply chain security (EO 14028, 2021). For example, the EO directed the National Institute for Standards and Technology (NIST), the nation's leading technology and cybersecurity standards agency, to create guidelines and recommendations for practices that improve the security and management of an organization's software supply chain—for example, by requiring software vendors to produce or provide a software bill of materials (SBOMs) as a way to reveal and document software dependencies across applications (NIST, 2022). In addition, NIST developed a taxonomy of critical software categories and functions and guidance concerning proper use and protection of these categories.

It also developed a set of minimums standards for vendors and developers regarding verification and testing of software, including third-party software.

In January 2022, in the wake of disclosure of the log4j software vulnerability, the White House convened a meeting of federal agencies, technology, and software companies to address the state of open-source software. The discussions concerned the growing acknowledgment of the role that open-source software plays in modern applications and supporting critical infrastructure. Afterward, the White House stated, "[s]oftware is ubiquitous across every sector of our economy and foundational to the products and services Americans use every day. Most major software packages include open source software" (White House, 2022). In response to the meeting, a Google executive stated,

> For too long, the software community has taken comfort in the assumption that open source software is generally secure due to its transparency and the assumption that "many eyes" were watching to detect and resolve problems. But in fact, while some projects do have many eyes on them, others have few or none at all (Walker, 2022).

These efforts highlight the extent and magnitude of the risks brought by software supply chain matters. Next, we examine how cybersecurity has been addressed at the SEC, both generally and in regard to one particular software issue (i.e., Year 2000 [Y2K]).

Two separate initiatives have prompted the collection of data and publishing of reports that unveiled the vastness and prevalence of open-source software usage through U.S. businesses and the intricate dependencies among these products.

SEC's Role in Mitigating Cyber Risk

The SEC has recognized cyber risk as a growing and important concern, and it has taken several steps to address it. In 2011, the SEC issued nonlegislative guidance concerning the disclosure of data breaches by publicly traded companies (SEC, 2011). The guidance stated that companies need to disclose a cyber incident if the issue makes investment speculative or risky, or if the incident represents an event that is reasonably likely to have a material effect on the firm's operations or financial condition. However, the guidance did not require disclosure of generic risks, those affecting everyone equally, or information that would jeopardize the firm's cybersecurity.

In updated guidance, the SEC stated,

> Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyberattack. (SEC, 2018, p. 17).

Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose "the most significant factors that make investments in the company's securities speculative or risky. Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among such factors, including risks that arise in connection with acquisitions" (SEC, 2018, p. 13).

Despite gaps in guidance around software supply chain risks, the SEC has created a portal to help investors and companies better understand cybersecurity and current threats, such as ransomware.

Furthermore, Item 101 of Regulation S-K and Item 4.B of Form 20-F require companies to "discuss their products, services, relationships with customers and suppliers, and competitive conditions. If cybersecurity incidents or risks materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company must provide appropriate disclosure" (SEC, 2018, p. 16).

In early 2022, the SEC also proposed additional rules regarding cybersecurity risk management, incident disclosure, and disclosure of the board of directors' cybersecurity experience (SEC, 2022). Of most relevance to this Perspective, the proposed SEC guidance would require a registrant to "[d]escribe its policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity as part of its business strategy, financial planning, and capital allocation" (SEC, 2022). Although software risk (specifically, software supply chain risks) might be included under the general theme of a cybersecurity threat, it is not specifically mentioned that proposal or elsewhere in SEC guidance.

Despite gaps in guidance around software supply chain risks, the SEC has created a portal to help investors and companies better understand cybersecurity and current threats, such as ransomware (SEC, undated). In addition, the SEC brings enforcement actions against companies for violation of its guidelines or other forms of fraud or transgressions. As of March 2022, it has initiated more than 150 enforcement actions related to digital assets or virtual currency, account intrusions, hacking, dark web activity, and other cyber issues.

So far, these efforts over the past 20 years are largely based around disclosure of cybersecurity incidents and ensuring that conventional forms of cybersecurity precautions are taken. However, none of the current SEC rules or regulations specifically address software supply chain risks, as described in this Perspective.

The SEC and Disclosure of Y2K Risks

Although the SEC may be reluctant to issue specific guidance on the disclosure of software applications, SEC has already provided guidance on software supply chain issues within the context of Y2K. Beginning in 1997, the SEC issued guidance regarding disclosure of potential software risks caused by improper date assignment for Y2K(SEC, 1998b). The Commission described the problem as follows (SEC, 1998a):

> Many existing computer programs use only two digits to identify a year in the date field. These programs were designed and developed without considering the impact of the upcoming change in the century. If not corrected, many computer applications could fail or create erroneous results by or at the Year 2000. The Year 2000 issue affects virtually all companies and organizations . . .
>
> As the end of this century nears, there is worldwide concern that Year 2000 technology problems may wreak havoc on global economies. No country, government, business, or person is immune from the potential far-reaching effects of Year 2000 problems . . .
>
> Many companies must undertake major projects to address the Year 2000 issue. Each company's potential costs and uncertainties will depend on a number of factors, including its software and hardware and the nature of its industry. Companies also must coordinate with other entities with which they electronically interact, both domestically and globally, including suppliers, customers, creditors, borrowers, and financial service organizations. If a company does not successfully address its Year 2000 issues, it may face material adverse consequences.

These passages clearly recognize and articulate the magnitude that software failure (either malicious or

As of March 2022, the SEC has initiated more than 150 enforcement actions related to digital assets or virtual currency, account intrusions, hacking, dark web activity, and other cyber issues.

accidental) could have on corporate business operations. Therefore, the Commission acknowledged the gravity of the risk and justified the need for disclosure to stakeholders about this risk (SEC, 1998b):

> We intend to intensify our efforts to elicit meaningful disclosure from companies about their Year 2000 issues. Only through that disclosure can investors make informed investment decisions. We believe that companies have sufficient incentive to provide meaningful disclosure to investors and meet their Year 2000 disclosure obligations. These incentives include business reasons, investor relations concerns, and possible referrals to our Division of Enforcement.
>
> SEC also stated (SEC, 1998b),
>
> For vendors and suppliers, the relationship is material if there would be a material effect on the company's business, results of operations, or financial condition if they do not timely become Year 2000 compliant. The same analysis should be made for significant customers whose Year 2000 readiness could cause a loss of business that might be material to the company. The company also should consider its potential liability to third parties if its systems are not Year 2000 compliant, resulting in possible legal actions for breach of contract or other harm. In our view, a company's Year 2000 assessment is not complete until it considers these third-party issues and takes reasonable steps to verify the Year 2000 readiness of any third party that could cause a material impact on the company.

Elements of Disclosure

In regard to the *content* of the required disclosure, the SEC stated (SEC, 1998b):

> We expect that for the vast majority of companies Year 2000 issues are likely to be material, and therefore disclosure would be required. When a company has a Year 2000 disclosure obligation, we believe that full and fair disclosure includes:
>
> (1) the company's state of readiness;
> (2) the costs to address the company's Year 2000 issues;
> (3) the risks of the company's Year 2000 issues; and
> (4) the company's contingency plans.

Scope of Disclosure

In regard to scope, the SEC recommended disclosure of a minimum of three components (SEC, 1998b):

- First, the discussion should address both information technology ("IT") and non-IT systems. Non-IT systems typically include embedded technology such as microcontrollers.
- Second, for both their IT and non-IT systems, companies should disclose where they are in the process of becoming ready for the Year 2000. The status of the company's progress, identified by phase, including the estimated timetable for completion of each remaining phase, is vital information to investors and should be disclosed.
- The third essential component is a description of a company's Year 2000 issues relating to third parties with which they have a material relationship. Due to the interdependence of computer

> systems today, the Year 2000 problem presents a unique policy issue. For example, if a major telecommunications company discloses that it may have a business interruption, this may require many other companies to disclose that they too may have a business interruption, if material.

Proposed Disclosure Guidelines

Building on previous Y2K disclosure rules, here we examine contemporary financial and SBOM disclosures for SEC consideration to promote increased management and transparency of software supply chain risk.

Managing Software Supply Chain Risk

First, the SEC could require that companies disclose their processes for managing their software supply chain risks. In particular, such disclosures could contain the following elements:

- Whether the company has a process for identifying, assessing, and mitigating software supply chain risks would need to be identified.
- A discussion of the scope of any software supply chain risk management efforts would be necessary. That is, an explanation of which business services have (and have not) been evaluated, and which business services are material to the company. The company must also describe whether it has accounted for all IT, embedded, hardware, and other software-dependent technologies.
- If the company plans not to manage software supply chain risks for one or more business services or components, it must provide an explanation describing why not.
- A high-level description of the results from any software supply chain risk assessment, discussed separately by business service, would be necessary. That is, if software supply chain risks for some business services have been completed, those assessments should be discussed separately from business services that have not been assessed. The disclosures "should be in sufficient detail to allow investors to fully understand the challenges that it faces. We suggest that the description be similar to that provided to a company's board of directors—which typically is non-technical plain English" (SEC, 1998b).

The SEC could require that companies disclose their processes for managing their software supply chain risks.

Although the SEC should require guidance around the disclosure of supply chain risks, the frameworks used and implemented in disclosing such guidance should be left to the individual organization. However, NIST has developed guidance concerning software supply chain management and risk disclosure (NIST, 2022). The management of software supply chain risks may also be assisted by developing, or requesting, software bill of materials (SBOM) of internal, and third-party software systems. As described in EO 14028, 2021,

> the term ‘Software Bill of Materials’ or ‘SBOM’ means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. . . . Those who operate software can use SBOMs to quickly and easily determine whether they are at potential risk of a newly discovered vulnerability. . . . Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.

Reliance on Critical Software Categories and IT Products and Services

As part of EO 14028, NIST was tasked with developing a list of critical software categories (EO14028, 2021). That is, software that is deemed to be essential to the proper and reliable operation of an organization’s computer network. These software applications may operate with elevated or administrative privileges to core computer networking devices (e.g., remote access and configuration management), perform or ensure critical security operations within a network (e.g., network protection, backup recovery and remote storage), or are ubiquitous applications that are often exposed to a heightened volume of software attacks (e.g., web browsers). Therefore, as a second consideration, the SEC could require companies to disclose where and under what circumstances the company uses software that

- has the ability to cause material harm to the organization if compromised or disrupted
- is included under the NIST definition of critical software (NIST, 2021).

Companies incur risks when using software developed by third parties, whether those software components are managed by commercial entities or open-source libraries.

Disclosing Risks From Third-Party Software Vendors

Companies incur risks when using software developed by third parties, whether those software components are managed by commercial entities or open-source libraries, and these risks are amplified whether dealing with major software providers or small but commonly used software libraries. For example, if a major software vendor, or cloud service provider discloses that it may have a business interruption, this may require many other companies to disclose that they too may incur a business interruption, if material. Thus, one company's software supply chain issues might affect other companies' disclosure obligations.

As a third consideration, as recommended by the SEC in its Y2K guidance (SEC, 1998c), in addition to disclosure of software management practices by the company, it might also be important for companies to request the software management practices of its software supply chain—again, whether from major software vendors or small open-source libraries. If a company is unable to obtain assurances about software management practices regarding a material relationship with a third-party software vendor or application (as is more likely for open-source software), a statement to that effect should be made.

For example, if a company buys or uses software from a sole supplier, and that sole supplier is unwilling or unable to disclose its software supply chain management practices, a statement to that effect should be made. Disclosure of the related contingency plan (e.g., in the event that the supplier has been compromised, such as switching to another supplier, and the ability to make such a switch) should also be discussed.

Companies may also disclose the nature and level of importance of these material relationships, as well as the status of assessing these third-party risks.

Conclusion

This Perspective has described a growing and important risk generated by the interdependency of a diverse number of software applications and components that run critical business services. Although the SEC has adopted numerous regulations and rules governing cybersecurity, none of those specifically, or adequately, speak to this risk.

We provided several disclosure options for SEC's consideration to promote increased management and transparency of software supply chain risk. For example, the SEC's Y2K disclosure requirements might serve as a useful model for developing appropriate and useful disclosure guidelines.

Although it is possible that the disclosure of specific software applications might create additional risks from malicious actors, more research should be conducted into qualifying any potential risks, because it may also be possible that any particular knowledge may not actually be valuable to a malicious actor.

Overall, we believe that increased disclosure of a company's software supply chain risks to investors will allow investors to better assess the overall management and cybersecurity protections employed by organizations.

References

EO 14028—*See* Executive Order 14028.

Executive Order 14028, "Improving the Nation's Cybersecurity," Washington, D.C.: *Federal Register*, Vol. 86, No. 93, May 12, 2021, pp. 26633–26647. As of May 16, 2022:
https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

Greig, Jonathan, "Log4J: Microsoft Discovers Attackers Targeting Undisclosed SolarWinds Vulnerability," ZDNet, January 21, 2022. As of May 16, 2022:
www.zdnet.com/article/log4j-microsoft-discovers-attackers-targeting-solarwinds-vulnerability/

Lee, Timothy B., "The Heartbleed Bug, Explained," Vox, June 19, 2014. As of May 16, 2022:
www.vox.com/2014/6/19/18076318/heartbleed

Nagle, Frank, Jessica Wilkerson, James Dana, and Jennifer L. Hoffman, *Vulnerabilities in the Core: Preliminary Report and Census II of Open Source Software*, San Francisco: Linux Foundation and the Laboratory for Innovation Science at Harvard, March 26, 2020.

National Institute of Standards and Technology, "Definition of Critical Software Under Executive Order (EO) 14028," October 13, 2021. As of May 16, 2022:
https://www.nist.gov/system/files/documents/2021/10/13/EO%20Critical%20FINAL.pdf

———, "Software Supply Chain Security Guidance: Purpose and Scope," webpage, last updated February 4, 2022. As of May 16, 2022:
www.nist.gov/itl/executive-order-improving-nations-cybersecurity/software-supply-chain-security-guidance-purpose

NIST—*See* National Institute of Standards and Technology.

SEC—*See* U.S. Securities and Exchange Commission.

Tan, Aaron, "Top Three Questions about the Log4j Vulnerability," ComputerWeekly.com, January 17, 2022, As of May 16, 2022:
www.computerweekly.com/news/252512071/Top-three-questions-about-the-Log4j-vulnerability

U.S. House of Representatives, Energy and Commerce Committee, "Walden, Harper Request Information on Open-Source Software - Energy and Commerce Committee," webpage, April 2, 2018. As of May 16, 2022:
https://republicans-energycommerce.house.gov/news/press-release/walden-harper-request-information-open-source-software/

U.S. Securities and Exchange Commission, "Cybersecurity," webpage, undated. As of May 16, 2022:
https://www.sec.gov/spotlight/cybersecurity

———, "Staff Legal Bulletin No. 5," January 12, 1998a. As of May 16, 2022:
www.sec.gov/interps/legal/slbcf5.htm

———, "SEC Interpretation: Disclosure of Year 2000 Issues and Consequences by Public Companies et Al," July 29, 1998b. As of May 16, 2022:
www.sec.gov/rules/interp/33-7558.htm

———, "SEC Interpretation: FAQ—SEC Statement Re Y2K Disclosure," November 9, 1998c. As of May 16, 2022:
www.sec.gov/rules/interp/33-7609.htm

———, "CF Disclosure Guidance: Topic No. 2—Cybersecurity," October 13, 2011. As of May 16, 2022:
www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

———, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 CFR Parts 229 and 249," February 26, 2018. As of May 16, 2022:
https://www.sec.gov/rules/interp/2018/33-10459.pdf

———, "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," Washington, D.C., press release, March 9, 2022. As of May 16, 2022:
www.sec.gov/news/press-release/2022-39

Veracode, *State of Software Security: Volume 11*, Burlington, Mass., 2020. As of May 16, 2022:
https://www.veracode.com/state-of-software-security-report--old2

Walker, Kent, "Making Open Source Software Safer and More Secure," *Google: The Keyword*, blog post, January 13, 2022. As of May 16, 2022:
https://blog.google/technology/safety-security/making-open-source-software-safer-and-more-secure/

White House, "Readout of White House Meeting on Software Security," webpage, January 14, 2022. As of May 16, 2022:
www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

About the Authors

Sasha Romanosky is a senior policy researcher at the RAND Corporation, an appointed Member of the Data Privacy and Integrity Advisory Committee at the Department of Homeland Security, and a former cyber policy adviser at the Pentagon in the Office of the Secretary of Defense for Policy. He researches the economics of cyber security, privacy, and national security. Romanosky holds a Ph.D. in public policy and management and a B.S. in electrical engineering.

Jonathan W. Welburn is a researcher at the RAND Corporation specializing in operations research and computational economics. His work has taken an interdisciplinary approach to model economic crises, supply chain risks, and cyber security. His current interests include systemic risks, cyber security, and policies for narrowing the racial wealth gap.

About This Perspective

The nation's reliance on computer software to run and manage critical business services has increased dramatically over many decades and only continues to grow. The increasing rate of and impact from the exploitation of software vulnerabilities have caused billions of dollars of damage and losses to thousands of companies across the world. Moreover, it has become increasingly true that modern software applications are built on a foundation of third-party and open-source software components, developed by thousands of professional and volunteer contributors across the world. This complexity and decentralized nature of the modern software ecosystem mean that firms are more separated from the oversight of the software that runs their businesses and increasingly exposed to risks because of this expanding software supply chain. Although many federal government agencies are vocal in addressing this issue in their own way, the U.S. Securities and Exchange Commission (SEC) has been relatively quiet. This Perspective presents a set of proposed disclosure rules that the SEC could implement to help address software supply chain security. This Perspective was conducted with support from RAND's Institute of Civil Justice and the Kenneth R. Feinberg Center for Catastrophic Risk Management and Compensation.

The RAND Kenneth R. Feinberg Center for Catastrophic Risk Management and Compensation seeks to identify and promote laws, programs, and institutions that reduce the adverse social and economic effects of catastrophes.

Acknowledgments

We would like to thank our reviewers, and RAND's Institute of Civil Justice and RAND's Kenneth R. Feinberg Center for Catastrophic Risk Management and Compensation for their generous support.

Institute for Civil Justice

The RAND Institute for Civil Justice (ICJ) is dedicated to improving the civil justice system by supplying policymakers and the public with rigorous and nonpartisan research. Its studies identify trends in litigation and inform policy choices concerning liability, compensation, regulation, risk management, and insurance. The Institute builds on a long tradition of RAND Corporation research characterized by an interdisciplinary, empirical approach to public policy issues and rigorous standards of quality, objectivity, and independence. ICJ research is supported by pooled grants from a range of sources, including corporations, trade and professional associations, individuals, government agencies, and private foundations. All its reports are subject to peer review and disseminated widely to policymakers, practitioners in law and business, other researchers, and the public. The ICJ is part of the Justice Policy Program within the RAND Social and Economic Well-Being Division. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.

RAND
CORPORATION

www.rand.org

For more information on this publication, visit www.rand.org/t/PEA2072-1.